CLAIMS

1. A computing environment, comprising:

a virtual machine;

a first application operating on said virtual machine; and

a first firewall control block, wherein said first firewall control block includes:

an associate security identification portion that identifies one or more associates of said first application as identified associates, and wherein each one of said one or more identified associates has access privilege with respect to said first application; and

an access-operations portion that for each one of said one or more identified associates identifies one or more operations that have been allowed to be performed.

2. A computing environment as recited in claim 1,

wherein said associate security identification comprises: one or more identifiers that have been assigned to said one or more identified associates; and

wherein for each one of said one identifiers, one or more operations have been defined in said access-operations portion.

3. A computing environment as recited in claim 2, wherein said one or more operations include read, write, delete, create, and update operations.

4. A computing environment as recited in claim 1,

wherein said computing environment includes a second application operating on said virtual machine,

wherein said first firewall control block includes a security ID of said second application, thereby indicating that said second application is an identified associate of said first application, and

wherein said first firewall control block also includes one or more operations that have been defined for said second application, thereby indicating what operations can be performed by said second application on said first application.

5. A computing environment as recited in claim 4,

wherein said computing environment is a Java™ compliant computing environment, and

wherein said first and second applications are Java™ compliant applets.

6. A computing environment as recited in claim 4,

wherein said computing environment is a Java Card™ compliant computing environment, and

wherein said first firewall control block is implemented in the run time environment.

7. A mobile computing device, comprising:

a Java™ compliant virtual machine;

a first Java™ compliant applet operating on said Java™ compliant virtual machine;

a first firewall control block, wherein said first firewall control block includes:

an associate security identification portion that identifies one or more associates of said first application as identified associates, wherein each one of said one or more identified associates has access privilege with respect to said first application, and

an access-operations portion that for each one of said one or more identified associates identifies one or more operations that have been allowed to be performed.

8. A mobile computing device as recited in claim 7, wherein said mobile device is a Java™ compliant smart card.

9. A mobile computing device as recited in claim 8, wherein a firewall control block is defined for every Java™ compliant applet that operates on said Java™ compliant virtual machine.

10. A method of providing security for a Java™ compliant computing environment that includes a Java™ virtual machine and a plurality of Java™ compliant applets that operate on said Java™ virtual machine, said method comprising:

receiving a request from a first Java™ compliant applet operating on Java™ virtual machine to perform an operation on a second Java™ compliant applet, said request including a security identifier that identifies said first Java™ compliant applet;

reading a firewall control block associated with said second Java™ compliant applet;

determining whether said firewall control block defines said security identifier as an associate of said second Java™ compliant applet; and

denying access to said first Java™ compliant applet when said determining determines that control block does not define said security identifier as an associate.

11. A method as recited in claim 10, wherein said method further comprises:

determining whether said firewall control block defines said operation as an operation that should be allowed when said determining determines that said firewall control block defines said security identifier as an associate; and

granting access to said first Java™ compliant applet to perform said operation on said second Java™ compliant applet when said determining determines that said firewall control block defines said operation as an operation that should be allowed.

12. A method as recited in claim 11, wherein said method further comprises:

providing a reference to said first Java™ compliant applet with a reference to said second Java™ compliant when access is granted.

13. A method as recited in claim 11, wherein said providing of a reference comprises:

invoking a first method that is implemented as a part of Java™ management (or system) environment; and

invoking a second method that is implemented as an applet class, as a result of said invoking of the second method.

14. A computing environment, comprising:

a virtual machine;

a first application operating on said virtual machine;

a second application operating on said virtual machine; and

a firewall control block, wherein said firewall control block includes one or more of the following:

a first firewall control block portion, wherein said first firewall control block portion defines access privileges of said first application with respect to said second application, and further defines the access privileges of said second application with respect to said first application.

a second firewall control block portion, wherein said second firewall control block portion includes:

an associate security identification portion that identifies one or more associates of said first application as identified associates, wherein each one of said one or more identified associates has access privilege with respect to said first application;

an access-operations portion that for each one of said one or more identified associates identifies one or more access operations that have been allowed.

15. A computing environment as recited in claim 14, wherein said first firewall control block portion includes a firewall control value and a firewall control indicator.

16. A computing environment as recited in claim 15,

wherein said firewall control value is an access privileges control value represented by one or more bytes, and

wherein said firewall control value is an indicator value represented by one or more bytes that indicate how the firewall control value should be interpreted with respect to access privileges of other applications.

17. A computing environment as recited in claim 14, wherein said first firewall control block portion includes a plurality of firewall control values and a plurality firewall control indicators.

18. A computing environment as recited in claim 14,

wherein said first firewall control block portion includes first and second firewall control values and first and second firewall control indicators, wherein the first firewall control value and indicator indicate access privileges of said first application to said second application, and

wherein said second firewall control value and indicator indicate access privileges of said second application to said first application.

19. A computing environment as recited in claim 14,

wherein said computing environment is a Java™ compliant computing environment, and

wherein said first and second applications are Java™ compliant applets.

20. A computing environment as recited in claim 18,

wherein said computing environment is a Java Card™ compliant computing environment, and

wherein said first firewall control block is implemented in Java Card™ run time environment.

21. A computing environment, comprising:

a virtual machine;

one or more applications operating on said virtual machine; and

one or more security context blocks provided for said one or more applications, wherein each of said one or more security context blocks include:

a security identification; and

a cryptographic system that can be used to perform cryptographic operations, wherein said cryptographic operations include cryptographic operations that can be performed on said security identification.

22. A computing environment as recited in claim 21,

wherein said security identification includes one or more security identifiers have been assigned to said one or more applications, and

wherein said cryptographic system includes:

one or more keys;

one or more key management information that provide information with respect said one or more keys; and

one or more algorithm identifiers that identify what cryptographic algorithm should be used.

23. A computing environment as recited in claim 22, wherein said cryptographic operations include digital signatures, verification, encryption, decryption, and authentication.

24. A computing environment as recited in claim 22, wherein said cryptographic system includes one or more cryptographic operation identifiers that identify one or more cryptographic operations associated with said one or more keys.

25. A computing environment as recited in claim 22, wherein said computing system further includes:

an encryptor that operates to encrypt a first string using one or more of said keys to generate an encrypted string;

a decryptor that operates to decrypt said encrypted string; and

a verifier that operates to determine whether the decrypted string can be verified..

26. A computing environment as recited in claim 22, wherein said computing environment further comprises:

a Java™ management applet that can operate to authenticate a security identification transmitted.

27. A method of providing security for a Java™ compliant computing environment that includes a Java™ virtual machine and a plurality of Java™ compliant applets that operate on said Java™ virtual machine, said method comprising:

providing a security context that includes a security identification and a cryptographic system;

receiving from a first Java™ compliant applet a request to perform an operation on a second Java™ compliant applet, wherein the request includes a first security identification

determining whether said first Java™ compliant applet can be authenticated; and

presenting the first security identification to said second Java™ compliant applet only when said determining determines that said first security identification can be authenticated.

28. A method as recited in claim 27, wherein said determining of whether said first Java™ compliant applet can be authenticated comprises:

verifying an encrypted string.

29. A method as recited in claim 27, wherein said determining whether said first Java™ compliant applet can be authenticated comprises:

sending a random string to said first Java™ compliant applet;

encrypting, by said first Java™ compliant applet, said random string to generate a encrypted string;

decrypting said random string to generate a decrypted string; and

determining whether said decrypted string matches said random string.

30. A method as recited in claim 27, wherein said authentication can be performed without a configuration file.

31. A method as recited in claim 27, wherein said authentication can be performed without user intervention.

32. A method of providing security in a Java™ compliant computing environment that includes a Java™ virtual machine and a plurality of Java™ compliant applets that operate on said Java™ virtual machine, said method comprising:

providing a cryptographic system for a first Java™ compliant applet, wherein said cryptographic system includes cryptographic keys, wherein said cryptographic keys are suitable for performing cryptographic operations using cryptographic algorithms; and

using, by said first Java™ compliant applet, said cryptographic, to perform a cryptographic operation on computer readable data; wherein said cryptographic operation is performed by said first Java™ compliant applet without user intervention.

33. A method of providing security in a Java™ compliant computing environment that includes a Java™ virtual machine, said method comprising:

providing a cryptographic system, wherein said cryptographic system includes cryptographic keys, and wherein said cryptographic keys are suitable for performing cryptographic operations using cryptographic algorithms; and

receiving a request from a first component to access a resource of said Java™ compliant computing environment; and

using said cryptographic system to perform at least one cryptographic operation to determine whether said first component should be granted access to said resource.

34. A method as recited in claim 33, wherein said first component is a host application that is attempting to access a resource.

35. A method as recited in claim 34, wherein said Java™ compliant computing environment is a Java Card™.

36. A method as recited in claim 33, wherein said first component is a Java™ applet.

37. A method as recited in claim 36, wherein said Java™ compliant computing environment is a Java Card™.